DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof. Reference herein to any social initiative (including but not limited to Diversity, Equity, and Inclusion (DEI); Community Benefits Plans (CBP); Justice 40; etc.) is made by the Author independent of any current requirement by the United States Government and does not constitute or imply endorsement, recommendation, or support by the United States Government or any agency thereof.

NATIONAL LABORATORY OF THE ROCKIES

DER Cybersecurity Standards

Assessment and Gap Analysis

Charles MaGill,[1] Danish Saleem,[1] Jordan Waggoner,[2] and Jenna deCastro [3]

1 National Laboratory of the Rockies
2 Idaho National Laboratory
3 Sandia National Laboratories

The National Laboratory of the Rockies is a national laboratory of the U.S. Department of Energy, Office of Critical Minerals and Energy Innovation, operated under Contract No. DE-AC36-08GO28308.

This report is available at no cost from the National Laboratory of the Rockies (NLR) at www.nrel.gov/publications.

Milestone Report
NLR/TP- 5C00-93100
January 2026

NATIONAL LABORATORY OF THE ROCKIES

DER Cybersecurity Standards

Assessment and Gap Analysis

Charles MaGill,[1] Danish Saleem,[1] Jordan Waggoner,[2] and Jenna deCastro [3]

1 National Laboratory of the Rockies
2 Idaho National Laboratory
3 Sandia National Laboratories

Suggested Citation
MaGill, Charles, Jenna deCastro, Danish Saleem, and Jordan Waggoner. 2026. DER Cybersecurity Standards: Assessment and Gap Analysis. Golden, CO: National Laboratory of the Rockies. NLR/TP- 5C00-93100. https://www.nrel.gov/docs/fy26osti/93100.pdf.

The National Laboratory of the Rockies is a national laboratory of the U.S. Department of Energy, Office of Critical Minerals and Energy Innovation, operated under Contract No. DE-AC36-08GO28308.

This report is available at no cost from the National Laboratory of the Rockies (NLR) at www.nrel.gov/publications.

Milestone Report
NLR/TP- 5C00-93100
January 2026

National Laboratory of the Rockies
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored in part by the National Laboratory of the Rockies for the U.S. Department of Energy (DOE), operated under Contract No. DE-AC36-08GO28308. Funding provided by the Grid Modernization Laboratory Consortium. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover photos (clockwise from left): Josh Bauer, National Laboratory of the Rockies 61725; Visualization from National Laboratory of the Rockies Insight Center; Getty-181828180; Agata Bogucka, National Laboratory of the Rockies 91683; Dennis Schroeder, National Laboratory of the Rockies 51331; Werner Slocum, National Laboratory of the Rockies 67842.

Acknowledgements

This report on Distributed Energy Resources (DER) Cybersecurity Standards was made possible through the collaborative efforts and support of numerous individuals and organizations. We extend our gratitude to the dedicated professionals from various standards development organizations, including IEEE, IEC, ISA, ISO, and UL, who have contributed their expertise and insights to the evolving landscape of DER cybersecurity. Special thanks to the industry stakeholders, utilities, manufacturers, and cybersecurity experts who participated in surveys, interviews, and working groups that informed this comprehensive gap analysis.

We are especially grateful to our Industry Advisory Board (IAB) for their invaluable guidance and feedback throughout the development of this document. In particular, we thank the members of the Smart Electric Power Alliance (SEPA), whose thoughtful review and consultation were instrumental in shaping the content and recommendations presented here. Their expertise and commitment to advancing DER cybersecurity standards greatly enriched this work.

The research team also acknowledges the significant contributions from key organizations such as the National Association of Regulatory Utility Commissioners (NARUC); the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER); and the Federal Energy Regulatory Commission (FERC), whose ongoing work continues to shape the cybersecurity standards for distributed energy resources. This report represents a collaborative effort to improve the security and resilience of our evolving electric grid, and we are grateful to all those who have contributed to this critical work.

List of Acronyms

- BES bulk electric system
- BESS battery energy storage systems
- BPS bulk power system
- CAGR compound annual growth rate
- CESER Office of Cybersecurity, Energy Security, and Emergency Response
- CIP Critical Infrastructure Protection
- CSF Cybersecurity Framework version 2.0
- DER distributed energy resource
- DERMS distributed energy resource management system
- DOE U.S. Department of Energy
- FERC Federal Energy Regulatory Commission
- GE General Electric
- IACS Industrial Automation and Control Systems
- IBR Inverter-Based Resource
- ICSP Interagency Committee on Standards Policy
- IEC International Electrotechnical Commission
- IEEE Institute of Electrical and Electronics Engineers
- INL Idaho National Laboratory
- IoT Internet of Things
- IT information technology
- NARUC National Association of Regulatory Utility Commissioners
- NATO CCDCOE North Atlantic Treaty Organization Cooperative Cyber Defense Centre of Excellence
- NERC North American Electric Reliability Corporation
- NIST The National Institute of Standards and Technology
- NLR National Renewable Energy Laboratory
- OT operational technology
- PV photovoltaic
- SNL Sandia National Laboratories
- UL Underwriters Laboratories

Executive Summary

The purpose of this report is to share the comprehensive gap analysis of existing cybersecurity standards applicable to distributed energy resources (DERs) within the electric power sector. This analysis aims to identify critical deficiencies in current standards, assess their alignment with industry needs, and provide actionable recommendations for enhancing cybersecurity measures. For the purposes of this report, DERs include both renewable and non-renewable resources, encompassing technologies that produce power (such as rooftop solar, battery storage, and backup generators) as well as those that consume or manage power (such as controllable thermostats, energy storage, and controllable electric vehicle charging). This definition covers resources located both behind the customer meter and those directly connected to the distribution grid .[1] The scope encompasses various DER technologies, including solar, wind, energy storage, and hydrogen fuel cell, and emphasizes the significance of establishing robust cybersecurity frameworks and standards to safeguard these increasingly integrated systems.[2] The report provides valuable insights for stakeholders in the DER ecosystem, including original equipment manufacturers, utilities, aggregators, and regulators. It underscores the importance of continued development and refinement of cybersecurity standards to keep up with the technical advances and new business models in DERs and aggregations thereof.

While this report provides recommendations for enhancing DER cybersecurity, it is important to note that a substantial and increasing share of DERs are owned and operated by individual customers and prosumers, who may lack the technical resources or regulatory obligations of traditional utilities or large aggregators. Many recommendations herein may not be practical or enforceable for these stakeholders, and the report highlights the need for tailored approaches and support mechanisms for customer-owned DERs. Furthermore, many such DERs operate outside formal regulatory or compliance regimes, posing unique challenges for grid security and oversight.

The analysis evaluated IEC, IEEE, ISA, ISO, and UL standards relevant to DER cybersecurity. Standards were assessed on their coverage of key requirements, including data availability, integrity, confidentiality, access control, and authentication, as well as the use of technical controls, such as encryption and system hardening, to support these functions. For each standard, the analysis assessed its alignment with current industry practices, regulatory compliance, effectiveness in addressing known risks, coverage of emerging risks, and how it promotes interoperability. The evaluation also considered potential integration challenges and barriers to adoption.

During the analysis, the team identified several gaps in existing cybersecurity standards that hinder the effective protection of DERs. Key findings from the analysis include:

1. **Inadequate coverage of DER-specific cybersecurity challenges:** Many standards were not originally designed with DERs in mind, leading to gaps in addressing DER-specific cybersecurity challenges that are discussed in more detail in Section 2.1. Many existing cybersecurity standards were developed before the widespread deployment of DERs and thus do not fully address their unique operational and security

[1] Danish Saleem, "Cybersecurity Standards for Distributed Energy Resources," *NLR.Gov*, n.d., https://www.NLR.gov/security-resilience/cybersecurity-standards.html.
[2] Saleem.

requirements relative to new business models and market structures driving their deployment. For example, standards like IEC 60870-5 and NERC CIP were designed for centralized, utility-scale systems and lack robust security features-such as strong authentication and encryption-that are necessary for geographically dispersed, internet-connected DERs[3]. These standards often fail to address vulnerabilities arising from localized attacks, bidirectional power flows, the complexities of securing distributed assets, the unique challenges of non-utility-owned devices, and the IT/OT convergence inherent in DER deployments.[4]

2. **Adoption challenges for newer standards:** Newer standards like IEEE 1547.3-2023 and UL 2941 are specifically designed to address DER cybersecurity but face significant adoption hurdles.[5] These include the need for substantial product redesigns, new interoperability standards, acquisition of specialized testing equipment, and workforce training to meet new requirements. Smaller manufacturers may find compliance particularly burdensome due to limited resources, while utilities and operators must adapt procurement and operational processes to align with these standards.[6]

   Section 2.2 elaborates on these adoption challenges, including financial, technical, and workforce barriers, and discusses the importance of industry collaboration and phased implementation to facilitate broader uptake of these critical standards

3. **Complexity in implementing comprehensive frameworks and standards:** Comprehensive frameworks such as ISA/IEC 62443 are recognized for their robust, holistic approach to industrial cybersecurity.[7] However, implementing these measures in DER environments can be complex, particularly since many DERs are owned and operated by individual ratepayers rather than organizations, who may have limited technical expertise and resources. The framework's requirements for defense-in-depth, lifecycle security management, and the integration of technological, process, and human factors can be resource-intensive and difficult to implement—especially given that many DERs are owned by individual consumers, who often lack the technical skills or resources typically available to organizations.[8]

   Section 2.3 details the specific complexities and offers recommendations for phased implementation and prioritization strategies to help organizations manage the complexity while enhancing security.

4. **Integration challenges with legacy systems:** Despite efforts to promote interoperability, integrating modern DER cybersecurity standards with legacy systems remains difficult.[9] Legacy equipment often

[3] Saleem.
[4] "Cyber Security for Distributed Energy Resources and DER Aggregators" (NERC, 2022), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf.
[5] "Privacy and Security Impacts of DER and DER Aggregators" (NERC, September 2023), https://www.nerc.com/comm/RSTC_Reliability_Guidelines/JointWhitePaper_PrivacyAndSecurityImpactsOfDERAggregators.pdf.
[6] Saleem, "Cybersecurity Standards for Distributed Energy Resources."
[7] "IEC 62443 Standard: An Overview" (Fortinet, n.d.), 62443, https://www.fortinet.com/resources/cyberglossary/iec-62443.
[8] "IEC 62443 Standard: An Overview," 62443.
[9] Jay Johnson and Danish Saleem, "Distributed Energy Resource (DER) Cybersecurity Standards" (NLR Cybersecurity & Resilience Workshop, Denver, CO, October 9, 2017), https://www.NLR.gov/docs/fy18osti/70454.pdf.

uses obsolete protocols and data formats, creating data silos and hindering real-time monitoring and secure communication. These systems may lack support for modern security features, increasing the attack surface and complicating compliance with current standards. Utilities frequently need to develop custom interfaces or undertake costly upgrades to bridge the gap between legacy and modern systems.[10]

Section 2.4 provides an in-depth analysis of these integration challenges, including technical, operational, and cybersecurity risks, and outlines best practices for retrofitting legacy DER installations

5. **Lack of harmonization between standards and regulatory requirements:** The absence of harmonized cybersecurity standards and regulatory requirements for DERs has resulted in a fragmented and inconsistent landscape.[11] While some federal requirements, such as NERC CIP, may apply to large aggregations of DERs, most DERs are subject to state-level regulation, if any regulation exists at all.[12] Consumer-owned, municipal, and cooperative systems often face little or no specific cybersecurity oversight.[13] This patchwork approach increases administrative complexity and can leave security gaps unaddressed. As states look to establish codified cybersecurity baselines for distribution system infrastructure, the lack of consistent terminology and requirements across existing standards and regulations can cause confusion, increase costs, and complicate efforts to develop effective and sensible regulation.[14]

   Section 2.5 provides concrete examples and discusses the impact of regulatory misalignment, referencing recent federal reports and industry feedback on how regulatory fragmentation increases compliance costs and harms cybersecurity outcomes.

This cybersecurity standards gap analysis underscores the urgent need for industry-wide collaboration in developing and refining comprehensive cybersecurity standards specifically tailored to DERs. Importantly, these standards must recognize and address the diverse roles and responsibilities of stakeholders, such as utilities, OEMs, and other entities acting as DER aggregators, since cybersecurity requirements may differ depending on who is fulfilling the aggregator function. By closing these gaps and accounting for stakeholder diversity, the report aims to promote a more resilient energy infrastructure capable of withstanding evolving cyber threats.

Building on the recommendations above, the report also suggests actions such as initiating an organized process for ongoing standards updates, promoting harmonization across existing standards to reduce compliance

[10] Johnson and Saleem.
[11] "Cybersecurity Baselines for Electric Distribution Systems and DER" (NARUC, February 2024), https://pubs.naruc.org/pub/35247A70-0C45-9652-C6D9-99A77C87200F?_gl=1*qhbmh7*_ga*MTA0MjA5NTEyNS4xNzI5NjA4NTc4*_ga_QLH1N3Q1NF*MTczMDI5NTQ4My4yLjAuMTczMDI5NTUxNS4wLjAuMA..
[12] "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid" (US Department of Energy, October 2022), https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf.
[13] Saleem, "Cybersecurity Standards for Distributed Energy Resources."
[14] Christina Simeone, "The Distribution Grid Gap on Cybersecurity," *Kleinman Center for Energy Policy* (blog), June 19, 2018, https://kleinmanenergy.upenn.edu/commentary/blog/the-distribution-grid-gap-on-cybersecurity/.

burdens, and enhancing guidance for integrating cybersecurity into current DER systems. These recommendations align with efforts like the SEI Energy Task Force (ETF), which has worked to establish ongoing updates and harmonization for grid standards, including specific profiles developed to address distributed energy resources (DERs) within the context of operational technology and cybersecurity. Additionally, the report emphasizes prioritizing development of standards that address emerging risks unique to distributed energy technologies.[15] By implementing these recommendations, stakeholders can improve the cybersecurity posture of DERs significantly, ensuring their safe integration into the evolving electric grid while mitigating potential vulnerabilities that could compromise energy infrastructure.[16]

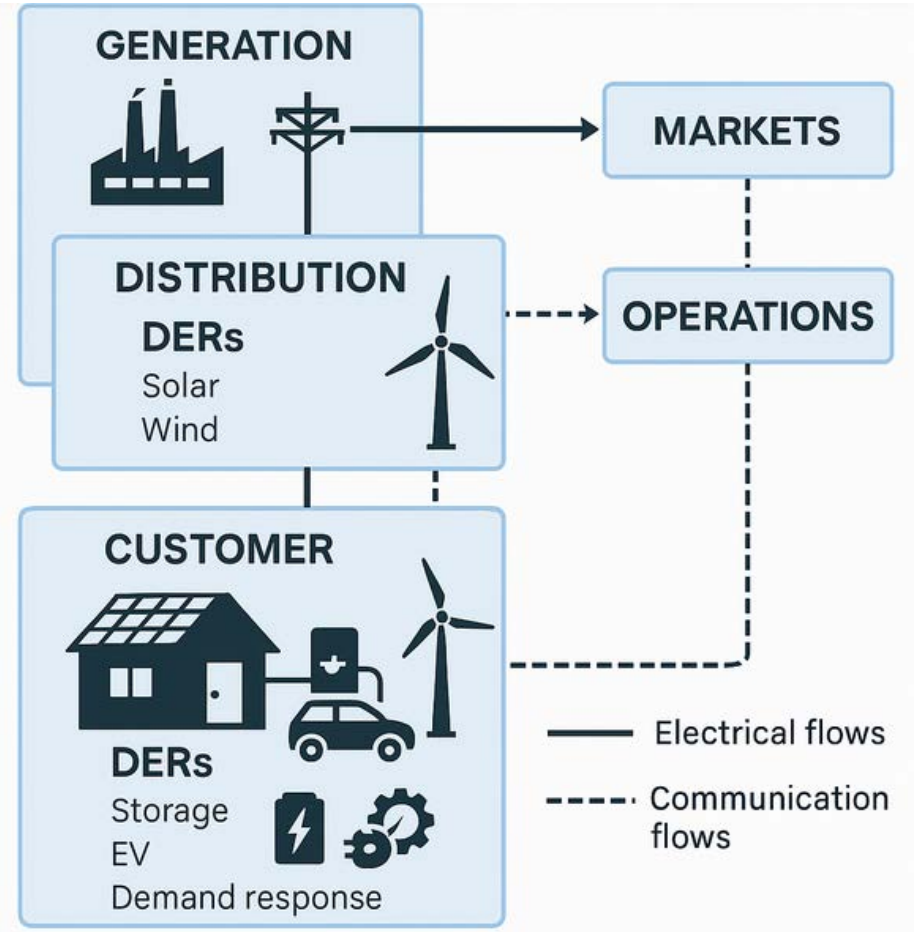

Figure 1. DER Domains and Interactions

Adapted from the NIST Smart Grid Interoperability Framework v4.0, this diagram illustrates DERs located in both the distribution and customer domains, highlighting their interactions with the grid and other energy management systems. (Figure by Charles MaGill / NLR).

[15] Saleem, "Cybersecurity Standards for Distributed Energy Resources."
[16] Saleem.

Table of Contents

1. Introduction 8
1.1 Standards Analyzed 9
1.2 Method for Analyzing DER Cybersecurity Standards 10
2. Gap Analysis - Identified Gaps 11
2.1 Inadequate coverage of DER-specific cybersecurity challenges 12
2.2 Adoption challenges for newer standards 14
2.3 Complexity in implementing comprehensive frameworks and standards 14
2.4 Integration challenges with legacy systems 15
2.5 Lack of harmonization between standards and regulatory requirements 16
3. Priorities for Harmonization and Closing Gaps 18
4. Conclusion 20
Bibliography 23
Appendix A: Standards Evaluated for Gap Analysis 26

1. Introduction

Distributed energy resources (DERs) are grid-edge devices that generate, store, or manage electricity, connected at the distribution level (typically ≤20 MW), and may be sited either on the utility distribution system or on customer premises. DERs include, but are not limited to, renewable and non-renewable distributed generation, energy storage systems, controllable loads, demand response, and electric vehicle charging infrastructure.

The main purpose of this gap analysis is to present a comprehensive evaluation of existing cybersecurity standards applicable to DERs and identify critical deficiencies that may hinder effective risk management against evolving cyber threats. This analysis evaluates effectively a comprehensive set of industry standards—specifically those established by leading organizations such as the International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), International Society of Automation (ISA), International Organization for Standardization (ISO), and Underwriters Laboratories (UL)—address the distinctive cybersecurity challenges presented by Distributed Energy Resources (DERs). The review highlights the roles of these organizations and the standards they develop, which are critical for ensuring the security and reliability of DER technologies.

The assessment focuses on essential cybersecurity aspects including data security, authentication, access control, and—importantly—privacy protections. Given that DERs and related customer-owned devices frequently handle sensitive information, privacy concerns are a central consideration. The analysis also examines the alignment of these standards with the current National Institute of Standards and Technology (NIST) Cybersecurity Framework version 2.0 (CSF), as well as the specific requirements and risks associated with distributed energy technologies.

DERs encompass a wide range of ownership and operational models, from utility-owned assets to those owned by third-party providers and, increasingly, individual ratepayers and prosumers. This diversity complicates the application of cybersecurity standards and regulatory requirements, as many customer-owned DERs fall outside traditional compliance regimes and may lack the resources or incentives to implement robust cybersecurity measures.

Harmonizing standards for DER technologies is of paramount importance in creating a secure ecosystem for the evolving energy sector. In this report, harmonization refers to the systematic process of mapping, aligning, and coordinating different cybersecurity standards and regulatory requirements to ensure interoperability, consistent interpretation, and reduced compliance complexity. Harmonization does not mean making all standards identical but rather focuses on identifying overlaps and differences in terms, concepts, and controls to facilitate integration and mutual understanding. The current landscape is characterized by a patchwork of standards and regulations from various organizations, which creates significant compliance burdens for DER manufacturers, utilities, aggregators and operators. This fragmented approach not only increases costs and complexity but also potentially leaves holes in cybersecurity coverage that malicious actors could exploit.

For example, the harmonization of IEC Common Information Model (CIM) with MultiSpeak focuses on mapping data models, identifying where terms and concepts are identical, closely matched, or require translation

between different terminologies and structures.[17] This approach allows for effective integration between systems even when the underlying standards were developed for different constituencies or use cases.

These gaps may arise due to several factors, starting with a lack of integration among disparate security tools, which can prevent effective communication and create blind spots in threat detection and response. Additionally, inconsistent policies across different systems can lead to vulnerabilities at the points where they intersect. Incomplete visibility is not merely a concern—it is an inevitable aspect of modern DER environments, given that utilities and original equipment manufacturers (OEMs) typically lack full oversight of non-utility owned and managed devices. This fragmented visibility means that security teams may struggle to detect and respond to critical indicators of compromise that could span across multiple platforms or devices outside their direct control. Moreover, managing multiple systems often results in delayed updates and patching, leaving known vulnerabilities exposed for longer periods. The complexity of overseeing numerous tools also increases the likelihood of human error, such as configuration mistakes or oversight. Finally, resource strain can hinder security teams' ability to effectively monitor and maintain these systems, potentially causing them to overlook crucial alerts or threats. Collectively, these gaps in coverage create opportunities for cybercriminals to exploit weaknesses, leading to data breaches, system compromises, or other security incidents that a more cohesive approach might have prevented.

By promoting harmonization, stakeholders can reduce redundancies, streamline compliance processes, and ensure a more consistent and comprehensive approach to DER cybersecurity. This unified approach is crucial for facilitating the secure integration of DERs into the broader energy ecosystem, supporting interoperability between dissimilar systems and enhancing the overall resilience of the electric grid in the face of increasingly sophisticated cyber threats. Addressing these gaps is crucial for ensuring that DERs can operate securely within the broader energy ecosystem while maintaining reliability and public trust.

1.1 Standards Analyzed

Figure 2 displays DER standards covering cybersecurity, safety, interconnection, and communication, as developed by leading organizations including IEC, IEEE, ANSI, ISA, and UL. The figure features a dedicated column highlighting cybersecurity standards, offering a focused overview of those specifically addressing cybersecurity. For this gap analysis, primary attention was given to the standards explicitly identified as cybersecurity-related in the first column. Nonetheless, the analysis also systematically reviewed each standard listed in Figure 1 to assess whether cybersecurity considerations are incorporated elsewhere within the broader

[17] G Gray, “Common Information Model (CIM)-MultiSpeak Harmonization 2nd Edition,” Technical (Palo Alto, CA: EPRI, Devcember 2012), https://restservice.epri.com/publicdownload/000000000001026585/0/Product.

standards. Subsection breakdowns are provided where relevant.

Figure 2. Key Standards Analyzed (Figure by Danish Saleem / NLR)

1.2 Method for Analyzing DER Cybersecurity Standards

The methodology for conducting this DER standards gap analysis involved a comprehensive and systematic approach to evaluate existing cybersecurity standards and their applicability to DERs. The process began with an extensive literature review, including academic publications, industry reports, regulatory documents, and technical standards. Key databases and repositories such as IEEE Xplore, IEC Standards, and NIST publications were systematically examined using relevant keywords related to DER cybersecurity. Additionally, industry feedback was gathered through meetings with an industry advisory board (IAB) developed specifically for this initiative, in addition to targeted surveys and interviews with other stakeholders across the DER ecosystem, including manufacturers, utilities, regulators, and cybersecurity experts. This multi-faceted approach ensured a holistic understanding of the current state of DER cybersecurity standards and practices.

The analysis was conducted against the NIST CSF. This approach was chosen because the NIST CSF is widely accepted framework that allowed for a systematic assessment of how well each standard addressed important cybersecurity requirements such as data confidentiality, integrity, availability, authentication, access control, and system hardening against a framework that is internationally recognized. The evaluation also considered the standard's alignment with current industry practices, regulatory compliance, and effectiveness in addressing known and emerging cybersecurity risks specific to DERs. Gaps were identified by comparing the coverage provided by existing standards against the comprehensive security requirements outlined in the NIST CSF, as well as considering the unique operational characteristics and vulnerabilities of DER systems.

A risk-based analysis was developed to prioritize the identified gaps and propose solutions. This considered factors such as the impact of a cyberattack, the likelihood of exploitation, and the feasibility of applying mitigations. Gaps were evaluated based on their criticality to the overall DER system security and the extent to which they left critical assets or functions vulnerable. The prioritization process also considered industry feedback on the most pressing cybersecurity challenges faced by DER operators and integrators. Proposed solutions were developed by analyzing the best practices from adjacent industries, emerging technologies, and cutting-edge research in cybersecurity. These solutions were then evaluated for their potential effectiveness, implementation complexity, and alignment with existing regulatory standards. The resulting prioritized list of gaps and proposed updates provides a roadmap for enhancing DER cybersecurity standards, focusing efforts on the most critical areas that require immediate consideration.

The standards that were analyzed as part of this process were also compiled into a library. The DER standards library was designed to aid researchers and developers alike by offering a singular platform for accessing and managing standards related to DERs. The library encompasses a swath of guidelines, reports, and other documentation researchers deemed crucial to ensure secure, efficient, and effective communications and cybersecurity within DER systems. The library is meant to be a central database for many standards that are relevant to DERs and is ultimately meant to simplify both the design and implementation of DER systems by enabling straightforward access to pertinent standards. The DER standards library also doubles as a historical archive, enabling users to retrieve older documents and references either for demonstrative or future analyses.[18]

2. Gap Analysis - Identified Gaps

The gap analysis used a methodical approach to identify areas where existing cybersecurity standards may fall short in addressing specific security needs. In the case of DERs, this analysis is particularly crucial due to the increasing integration of renewable energy sources into the power grid, which introduces new vulnerabilities and challenges. The standards gap analysis leveraged the NIST CSF, a widely recognized and comprehensive guide for managing and reducing cybersecurity risks. This framework provides a structured approach to cybersecurity, organizing best practices into six core functions: Govern, Identify, Protect, Detect, Respond, and Recover.[19] By using this framework as a benchmark, the research systematically evaluated the effectiveness of existing standards in addressing DER cybersecurity concerns.

This process involved a detailed examination of how well current standards align with each of the CSF's core functions, pinpointing areas where standards may be lacking or insufficient. The resulting analysis not only highlights gaps in coverage but also provides a foundation for developing more robust and comprehensive cybersecurity standards tailored to the unique challenges posed by DER systems. The subsequent information delves deeper into these identified gaps, offering a more nuanced understanding of where improvements are needed to enhance the security posture of DER implementations.

[18] DER Standards Library: https://apps.openei.org/der-cyber-standards/
[19] "The NIST Cybersecurity Framework (CSF) 2.0" (NIST, February 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

For clarity, all references to DERs in this section use the standardized definition provided in the Introduction and Glossary, unless otherwise specified by the cited standard.

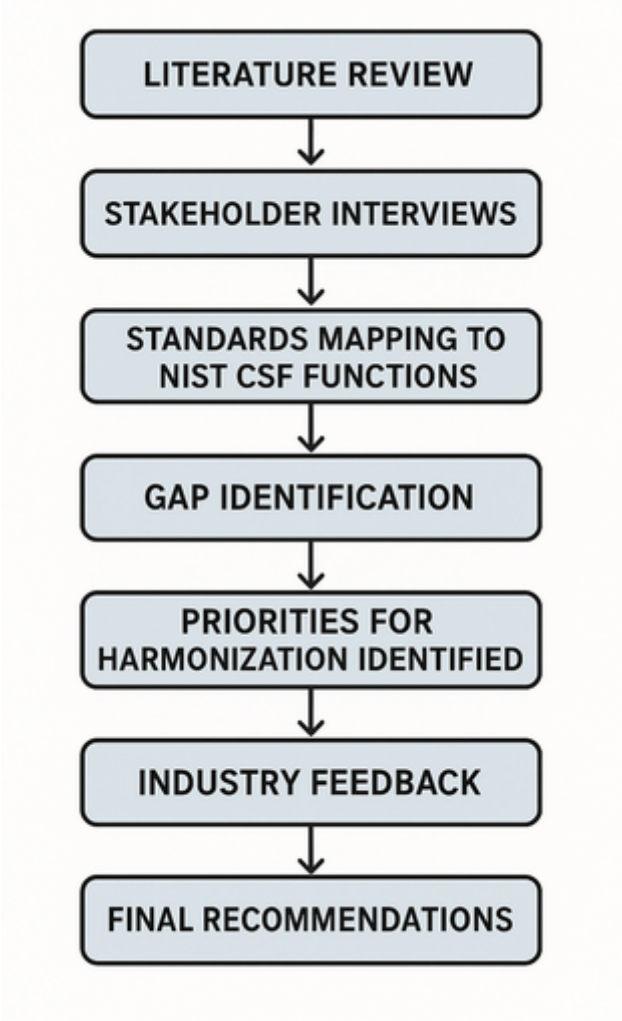

Figure 3. DER Cybersecurity Standards GAP Analysis Methodology

(Figure by Charles MaGill / NLR).

2.1 Inadequate coverage of DER-specific cybersecurity challenges

Based on the research team's analysis, existing power industry standards, developed before many smart grid technologies, have notable cybersecurity gaps. Based on the research team's analysis of IEC 60870-5 and NERC CIP, these standards were designed for centralized electric systems and lack robust security measures for distributed resources.[20]

[20] "SECURING DISTRIBUTED ENERGY RESOURCES" (NIST, n.d.), https://www.nccoe.nist.gov/sites/default/files/legacy-files/es-iiot-fact-sheet.pdf.

These standards fail to address key DER-specific challenges, such as:

- Vulnerability to localized and targeted attacks: Unlike traditional utility assets, DERs may be exposed to physical and cyber risks at individual sites, with potential impacts on distributed customers and the broader grid.
- Complexities of securing geographically dispersed and varied ownership models: DERs are frequently owned and managed by a mix of utilities, third-party providers, and end customers, complicating oversight and coordination compared to centralized transmission infrastructure.
- Bidirectional power flow and communication risks: DERs introduce new vectors for cyber threats due to two-way electricity and data flows, unlike the more predictable, unidirectional systems in traditional transmission.
- Software supply chain management challenges: The proliferation of software and firmware across diverse DER devices raises concerns about supply chain integrity, secure updates, and vulnerability management.
- Cloud adoption and integration risks: Increasing reliance on cloud-based platforms for monitoring and control of DERs introduces additional security considerations around data privacy, access control, and system resilience.
- Distinct challenges compared to transmission utilities: While transmission utilities also manage large, dispersed assets, DERs present unique security concerns due to their scale, diversity, and the involvement of non-utility owners and operators.

Continuing with the example of IEC 60870-5, this standard provides a foundational protocol for SCADA systems but lacks the robust security and authentication mechanisms required for securing distributed energy resource installations, making it vulnerable to unauthorized control and data manipulation compared to its more secure application within the confines of a traditional substation environment. For instance, the protocol's limited encryption and reliance on polling-based communication introduce vulnerabilities that are easily exploitable in the geographically dispersed modern DER systems, posing a risk to grid stability.

While newer standards such as IEEE 1547.3-2023 and UL 2941 are designed to address existing gaps, their implementation is complicated by several factors. These include the need for significant system modifications and the potential for regulatory misalignment. Although DERs themselves are often not subject to traditional utility regulation, inconsistencies can arise when standards overlap with or are interpreted differently by, local, state, or federal authorities, especially where existing grid codes or interconnection requirements are involved. This regulatory uncertainty may create obstacles to uniform adoption and enforcement of the latest security standards. The industry is currently working to integrate these DER-specific cybersecurity standards with existing standards while addressing emerging security risks.[21]

[21] Steven Brewster, "UL Solutions and NLR Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification Requirements," *UL Solutions*, April 18, 2023, https://www.ul.com/news/ul-solutions-and-NLR-announce-distributed-energy-and-inverter-based-resources-cybersecurity.

2.2 Adoption challenges for newer standards

As reported by UL Solutions and NLR, IEEE 1547.3-2023 and UL 2941 are newer standards for DER cybersecurity[22]. IEEE 1547.3-2023 makes available comprehensive guidelines for risk assessment, network security, access control, and data protection in distributed energy systems.[23] UL 2941 establishes testable cybersecurity requirements for DERs and inverter-based resources, including PV inverters, EV chargers, and wind turbines. These standards look to promote security by design principles, ensuring that cybersecurity measures are integrated into DER systems from initial concept and design.

However, these new standards pose significant implementation challenges for manufacturers.[24] Compliance may necessitate significant product redesigns, which may drive up development costs and lengthen production time as companies adapt to satisfy new cybersecurity requirements. For instance, small DER manufacturers can face hurdles in adopting IEEE 1547.3-2023, including the high cost of acquiring specialized testing equipment needed to validate compliance and the challenge of securing or training staff with the necessary cybersecurity expertise.[25] These financial and technical barriers can disproportionately impact smaller companies, potentially slowing down the overall adoption of critical cybersecurity measures within the DER industry.

Utilities and DER operators may also face difficulty in integrating these new standards into their existing procurement and operational processes.[26] The lack of familiarity with these new standards among industry professionals could further slow adoption, as there may be a learning curve associated with understanding and implementing the new requirements.

While implementing these standards presents challenges, their adoption is essential. As DERs become more integrated into the power grid, robust cybersecurity measures are increasingly important to protect these infrastructure components. These standards provide a unified approach to DER cybersecurity, which can help reduce vulnerabilities and improve overall grid resilience. To facilitate adoption, industry stakeholders, including manufacturers, utilities, and regulators, will need to collaborate closely.[27] This may involve providing training and resources to help organizations understand, prioritize, and implement the new standards, as well as potentially phasing in requirements over time to allow for a smoother transition.

2.3 Complexity in implementing comprehensive frameworks and standards

ISA/IEC 62443 provides a comprehensive cybersecurity framework for industrial automation and control systems,[28] offering structured guidance for securing DER systems throughout their lifecycle. While its holistic approach to technological, process, and human factors makes it valuable for complex DER environments,

[22] Brewster.
[23] Brewster.
[24] Kelsey Misbrener, "New UL Certification Works to Protect Solar Inverters from Cyberattacks," *Solar Power World* (blog), October 1, 2024, https://www.solarpowerworldonline.com/2024/10/new-ul-certification-solar-inverters-cyberattacks/.
[25] "Protecting Our Power: Cybersecurity Standards for Distributed Energy Resources," *IEEE SA*, December 12, 2024, https://standards.ieee.org/beyond-standards/cybersecurity-standards-der/.
[26] "Privacy and Security Impacts of DER and DER Aggregators."
[27] "Privacy and Security Impacts of DER and DER Aggregators."
[28] "What Is IEC 62443?," in *Zpedia* (zscaler, n.d.), https://www.zscaler.com/zpedia/what-is-iec-62443.

implementation poses significant challenges, particularly for smaller organizations with limited resources and technical expertise.[29]

The evolving energy sector introduces a complex array of cybersecurity standards from multiple authorities, but the primary compliance challenge for DER stakeholders arises from the differing regulatory and compliance regimes that accompany these standards. Since distribution systems, and by extension, many DERs are regulated at the state level, each state can establish its own unique security and compliance requirements. For DER owners and operators who operate across multiple states, this patchwork of regulations makes it difficult to maintain a consistent and effective security policy, often forcing them to adopt the least common denominator approach to compliance. To address these challenges, organizations should adopt a phased implementation approach, prioritizing critical areas through strategic risk assessments and leveraging specialized tools like OT zero trust solutions.[30]

2.4 Integration challenges with legacy systems

DER standards promote interoperability through common methodologies and terminology, enabling seamless integration of DER systems with the electric grid. IEEE 1547-2018 specifies technical requirements for DER interconnection and interoperability with utility power systems, setting uniform standards, requirements for performance, operation, testing, safety, and maintenance.[31] IEEE 2030.5-2018 integrates TCP/IP, HTTP, and TLS to manage end-user energy systems, including distributed generation, demand response and load control. These standards create best practices for manufacturers, utilities, and operators to develop compatible systems.[32]

As described by Liam Critchley in "Old Becomes New: Retrofitting Legacy Equipment for Smart Grid", despite efforts to promote interoperability, integrating legacy systems with modern smart grid technologies remains hard to achieve.[33] Obsolete protocols and data formats create data silos and hinder sharing capabilities, while the lack of real-time monitoring features necessitates complex middleware or costly upgrades. Cybersecurity problems are significant risks, as legacy systems increase vulnerability to attacks and increase the grid's attack surface, often failing to comply with current security standards.[34] Utilities often need to develop custom interfaces or adapters, implement gradual system upgrades, and adopt future-proof technologies that can work with both legacy and modern components. This process requires careful planning and significant investment to ensure seamless integration and maintain grid security.

Enhancing the integration of cybersecurity measures into legacy DER systems can be achieved through a phased approach. These practices, including conducting comprehensive risk assessments to identify vulnerabilities,

[29] "Cybersecurity Baselines for Electric Distribution Systems and DER."
[30] Jennifer Tullman-Botzer, "How to Overcome the Top Challenges of OT Security with Zero-Trust Access," *Cyolo* (blog), August 15, 2023, https://cyolo.io/blog/how-to-overcome-ot-security-challenges-with-zero-trust-access.
[31] David Narang, "Highlights of IEEE Standard 1547-2018 Implementation Considerations," https://www.NLR.gov/docs/fy21osti/81028.pdf.
[32] Mark Siira, William Rubin, and Rudi Schubert, "IEEE Standards for the Evolving Distributed Energy Resources (DER) Ecosystem," *IEEE SA*, November 9, 2021, https://standards.ieee.org/beyond-standards/ieee-standards-for-the-evolving-distributed-energy-resources-der-ecosystem/.
[33] Liam Critchley, "Old Becomes New: Retrofitting Legacy Equipment for Smart Grid," *EE Power* (blog), May 14, 2024, https://eepower.com/tech-insights/old-becomes-new-retrofitting-legacy-equipment-for-smart-grid/#.
[34] Critchley.

implementing network segmentation to protect critical systems, deploying intrusion detection to monitor for threats, and applying timely security patches, are recognized security best practices. However, their broad feasibility for DERs may be limited by factors such as device heterogeneity, resource constraints, and the lack of direct control over customer-owned assets. Additionally, the extent to which these measures are effectively implemented depends heavily on how securely OEMs manage their software supply chains and provide ongoing support for updates and vulnerability management. Additional considerations include upgrading communication protocols, implementing stronger authentication mechanisms, and providing cybersecurity training to personnel.

2.5 Lack of harmonization between standards and regulatory requirements

Within this report, harmonization is defined as the process of aligning and mapping different cybersecurity standards and regulatory requirements to ensure a common understanding and approach. This involves documenting where terms, requirements, or controls overlap, differ, or require translation between standards, supporting effective integration and reducing the risk of conflicting or redundant compliance obligations. Harmonization is an ongoing process, adapting as new technologies and regulations emerge.

As noted by Jonathan Reed in "Regulatory Harmonization in OT-Critical infrastructure Faces Hurdles", the lack of harmonization in cybersecurity standards and regulatory requirements is a significant issue affecting various sectors of the economy, particularly critical infrastructure.[35] This disjointed regulatory environment creates several challenges, including increased compliance burdens and potentially compromised cybersecurity effectiveness. Organizations face a complex web of overlapping and sometimes conflicting regulations from federal, state, and international authorities, forcing them to allocate substantial time and resources towards compliance.[36] This diversion of efforts could otherwise be used for enhancing cybersecurity measures and IT upgrades. The lack of harmonization and reciprocity increases compliance costs, which can be particularly burdensome for smaller organizations.[37]

Most customer-owned DERs operate outside the direct jurisdiction of federal or state cybersecurity regulations, such as NERC CIP or FERC orders. As a result, compliance-based approaches may be ineffective for this segment. Addressing cybersecurity for these DERs will require alternative strategies, such as voluntary standards, incentives, or market-based mechanisms that encourage adoption of best practices without imposing undue burdens on individual owners.

The proliferation of disjointed regulations has led to a fragmented approach to cybersecurity, potentially leaving gaps in security coverage. While regulatory compliance imposes important administrative requirements that are critical and foundational to effective cybersecurity, balancing these obligations with operational activities is essential to achieving optimal security outcomes. Additionally, a disjointed regulatory environment can be inflexible and risk stifling innovation in cybersecurity practices. Recognizing these challenges, both government and industry stakeholders are pushing for regulatory harmonization. The Office of the National Cyber Director (ONCD) is developing a comprehensive policy framework for regulatory harmonization, while legislation like the

[35] Jonathan Reed, "Regulatory Harmonization in OT-Critical Infrastructure Faces Hurdles," *IBM*, June 17, 2024, https://www.ibm.com/think/news/regulatory-harmonization-ot-critical-infrastructure-hurdles.
[36] Reed.
[37] Reed.

proposed Cybersecurity Regulatory Harmonization Act aims to establish an interagency "Harmonization Committee" to align cybersecurity regulations across agencies. Many industry sectors broadly support the need for enhanced cybersecurity regulation but advocate for better alignment among regulatory agencies.[38]

To solve these harmonization issues, several potential solutions have been proposed. These include developing a national baseline cybersecurity framework that can be leveraged across sectors, implementing a system of mutual recognition between regulators to reduce redundant compliance efforts, and engaging with like-minded allies to harmonize cybersecurity laws and policies across borders.[39] The goal is to strengthen cybersecurity resilience across critical infrastructure sectors while reducing the administrative burden and cost on regulated entities.[40] Harmonization efforts, such as those between IEC CIM and MultiSpeak, demonstrate that effective alignment is achieved through mapping and correlation-not by enforcing identical language. These initiatives document where standards overlap, where data transformations are needed, and where gaps exist, providing practical guidance for utilities and vendors integrating products based on different standards.[41] Such mapping exercises also reveal cases where different terms are used for the same concept, or where the same term may have different meanings, which is critical for avoiding misinterpretation and ensuring robust integration.

[38] Matt Seldon, "Office of the National Cyber Director Releases Summary of 2023 Cybersecurity Regulatory Harmonization Request for Information," June 11, 2024, https://www.hstoday.us/subject-matter-areas/cybersecurity/office-of-the-national-cyber-director-releases-summary-of-2023-cybersecurity-regulatory-harmonization-request-for-information/.
[39] Megan Brown et al., "Calls for Cybersecurity Regulatory Harmonization Ramp Up in Congress, White House," *Wiley* (blog), June 7, 2024, https://www.wiley.law/alert-Calls-for-Cybersecurity-Regulatory-Harmonization-Ramp-Up-in-Congress-White-House.
[40] Megan Brown et al., "CYBER UPDATE: White House Seeks Regulatory Harmonization While Exploring a Pilot for Reciprocity Amid Proliferation of Regulations," *Wiley*, June 5, 2024, https://www.wiley.law/alert-CYBER-UPDATE-White-House-Seeks-Regulatory-Harmonization-While-Exploring-a-Pilot-for-Reciprocity-Amid-Proliferation-of-Regulations.
[41] Gray, "Common Information Model (CIM)-MultiSpeak Harmonization 2nd Edition."

3. Priorities for Harmonization and Closing Gaps

Harmonization should be understood as an ongoing process of mapping and alignment rather than as an effort to make all standards identical in language or structure. This process involves first identifying where terms and concepts are either identical or closely matched across different standards. It also requires careful documentation of instances where different terms are used to describe the same concept, or conversely, where the same term may be applied with different meanings in separate standards. To support clarity and interoperability, harmonization efforts should include the development of reference mappings and companion documents that explicitly outline these relationships and distinctions. As new technologies and standards continue to emerge, it is important to recognize that harmonization is not a one-time task but a continuous effort, ensuring that standards remain aligned and relevant in a rapidly evolving landscape. Based on the findings of this analysis, the research team recommends the following actions:

1. Build on existing collaborative efforts, such as those led by NARUC, which has already established cybersecurity baselines for distribution systems and DERs to promote consistent security practices. Continue to foster coordination among standards organizations, industry stakeholders, and regulatory bodies, aiming to refine a common taxonomy and shared risk assessment methodology across standards and technologies. Additionally, prioritize the development and updating of standards to address emerging risks, including those introduced by AI and machine learning in DER applications, to ensure the cybersecurity landscape remains robust and forward-looking.[42]

2. Promote interoperability and secure communication protocols across different DER systems and grid infrastructure. This vital step for creating a cohesive and resilient energy ecosystem can be achieved by further developing and refining standards like IEC 60870-5 series and IEC 62351, ensuring they adequately address the specific communication needs and security challenges of diverse DER technologies.

3. Enhance the integration of cybersecurity measures into legacy DER systems. This can be achieved by developing specific guidelines and best practices for retrofitting existing installations with modern security features, ensuring that older systems do not become vulnerable entry points for cyber-attacks.[43]

4. Promote both security by design and security by default in the development and deployment of Distributed Energy Resources (DERs), building on initiatives like CIE and standards such as IEC 62351.[44] This approach is essential not only for utility-owned DERs but also for those managed by other stakeholders, helping to minimize vulnerabilities and enhance system resilience.

5. Build on efforts like the SEI ETF working group's "profiles" by developing technology-specific annexes or companion standards that address unique challenges, while leveraging foundational standards such as

[42] Jamie Lian, Teja Kuruganti, and Yan Liu, "Artificial Intelligence Tools Secure Tomorrow's Electric Grid," July 22, 2024, https://www.ornl.gov/news/artificial-intelligence-tools-secure-tomorrows-electric-grid.
[43] "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid."
[44] "IEC 62351 – Cyber Security Series for the Smart Grid" (IEC, Active), 62351, https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/.

IEEE 1547.3-2023.[45] These tailored guidelines should address the unique operational characteristics and vulnerabilities of several DER types, including wind turbines, solar PV, and energy storage systems.

6. Define a structured process for ongoing standards updates is crucial to keep up with the changing threat landscape and technological advancements in the DER sector.

By implementing these recommended actions, the industry can make significant strides in harmonizing standards, closing critical gaps, and enhancing the overall cybersecurity posture of DERs in the evolving electric grid.

[45] "Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems" (IEEE SA, n.d.), https://sagroups.ieee.org/scc21/standards/ieee-std-1547-3-2007-revision-in-progress/.

4. Conclusion

Comprehensive analysis of cybersecurity standards for DERs has revealed notable gaps that should be addressed to ensure the security and reliability of these increasingly integrated systems. Key findings indicate that many existing standards were not originally designed with DERs in mind, leading to insufficient coverage of DER-specific cybersecurity challenges. While newer standards like IEEE 1547.3-2023 and UL 2941 offer more targeted approaches to DER cybersecurity, they face adoption challenges due to their recent introduction. The analysis also highlighted the complexity of implementing comprehensive standards like ISA/IEC 62443 in DER systems, particularly for smaller organizations with limited resources.[46]

One critical issue identified is the lack of harmonization between standards and regulatory requirements, which increases compliance burdens and potentially compromises overall cybersecurity effectiveness. This fragmented approach not only increases costs and complexity but also potentially leaves gaps in cybersecurity coverage that malicious actors could exploit. Furthermore, while many standards promote interoperability by providing common standards and terminology, integration challenges remain, particularly with legacy systems.

Harmonization of standards should be viewed as an ongoing process of mapping and alignment, rather than an attempt to make all standards identical in language or structure. This approach begins with identifying where terms and concepts overlap or diverge across different standards, carefully documenting instances of synonymous terminology or differing definitions for the same term. To enhance clarity and interoperability, harmonization efforts should include the creation of reference mappings and companion documents that explicitly outline these relationships and distinctions. Recognizing that new technologies and standards are continually emerging, harmonization must be treated as a continuous effort to keep standards aligned and relevant. To address key gaps in DER cybersecurity and promote alignment, several critical actions are recommended: establishing coordinated efforts among standards organizations, industry, and regulators to develop common taxonomies and risk assessment methodologies; enhancing cybersecurity integration in legacy systems through retrofit guidelines; encouraging security by design as outlined in standards like IEC 62351;[47] developing technology-specific annexes to foundational standards such as IEEE 1547.3-2023;[48] defining structured processes for ongoing standards updates; and promoting interoperability and secure communication protocols through further development of standards like IEC 60870-5 and IEC 62351.[49] By pursuing these actions, the industry can make significant progress in harmonizing standards, addressing critical gaps, and strengthening the cybersecurity of DERs within the evolving electric grid.

Given the diversity of DER ownership, recommendations should be tailored to reflect the different capabilities and regulatory obligations of each stakeholder group. For customer-owned DERs, simplified cybersecurity guidance, technical support, and incentive programs may be more effective than compliance mandates. Further research and engagement with ratepayers, small businesses, and community organizations are needed to develop practical solutions that enhance security without imposing excessive burdens. The findings highlight

[46] "IEC 62443 Standard: An Overview," 62443.
[47] "Cyber Security: Understanding IEC 62351," January 23, 2023, https://www.iec.ch/blog/cyber-security-understanding-iec-62351.
[48] Thomas Basso and B Kroposki, "IEEE 1547.1 Overview" (Golden, Colorado, October 14, 2004), https://www1.eere.energy.gov/solar/pdfs/15a_1547_1.pdf.
[49] "Cyber Security: Understanding IEC 62351."

critical cybersecurity challenges in DERs that demand immediate industry-wide action. To promote alignment across standards and address key gaps in DER cybersecurity, a coordinated effort among standards organizations, industry stakeholders, and regulatory bodies is essential to harmonize existing standards and develop a unified framework for DER cybersecurity. Gathering feedback from multiple partners has proven challenging. Future efforts could benefit from employing more structured feedback mechanisms, such as targeted surveys with incentives for participation, or establishing smaller, dedicated advisory groups with regular meeting schedules. Continuous improvement is important as well to maintain the harmonization of DER cybersecurity standards far into the future.

Glossary

Term	Definition
Bulk Electric System	The interconnected electrical components and systems that make up the core of the electric grid, typically at high voltage, excluding local distribution.
Battery Energy Storage Systems	Systems that store electrical energy in batteries for later use, often used to balance supply and demand or provide backup power.
Bulk Power Systems	The large-scale electrical generation and transmission system, including generation plants and high-voltage transmission lines, but not local distribution networks.
Critical Infrastructure Protection	A set of standards developed by NERC to protect the assets vital to the operation of the bulk electric system from cyber and physical threats.
Cybersecurity Framework	A widely accepted set of guidelines and best practices developed by NIST to manage and reduce cybersecurity risk, structured around five core functions: Identify, Protect, Detect, Respond, Recover.
Distributed Energy Resource	Any resource capable of generating, storing, or managing electricity, connected at the distribution level (≤20 MW), including both renewable and non-renewable sources, and sited either on the utility distribution system or on customer premises.
Harmonization	The systematic process of mapping, aligning, and coordinating different standards and regulatory requirements to ensure interoperability, consistent interpretation, and reduced compliance complexity. In the context of DER cybersecurity, harmonization focuses on identifying and documenting overlaps and differences among standards to facilitate integration and mutual understanding, without requiring all standards to use identical language or structure.

Term	Definition
Inverter Based Resource	A type of DER that connects to the grid through power electronic inverters, such as solar PV systems, wind turbines, and battery storage.
International Electrotechnical Commission	A global organization that prepares and publishes international standards for electrical, electronic, and related technologies.
Institute of Electrical and Electronics Engineers	A professional association that develops standards for electrical, electronic, and computing technologies, including DER interconnection and cybersecurity.
Internet of Things	A network of interconnected devices that collect and exchange data, often used in DER systems for monitoring and control.
Operational Technology	Hardware and software that detects or causes changes through direct monitoring and control of physical devices, processes, and events in industrial environments.
Photovoltaic	A technology that converts sunlight directly into electricity using semiconductor materials.
Role-Based Access Control	A security approach that restricts system access to authorized users based on their roles within an organization.
Transport Layer Security	A cryptographic protocol designed to provide secure communication over a computer network, widely used to encrypt data transmitted by DERs.
Zero Trust	A cybersecurity model that requires strict verification for every user and device attempting to access resources, regardless of whether they are inside or outside the network perimeter.

Bibliography

Basso, Thomas, and B Kroposki. “IEEE 1547.1 Overview.” Golden, Colorado, October 14, 2004. https://www1.eere.energy.gov/solar/pdfs/15a_1547_1.pdf.

Brewster, Steven. “UL Solutions and NLR Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification Requirements.” *UL Solutions*, April 18, 2023. https://www.ul.com/news/ul-solutions-and-NLR-announce-distributed-energy-and-inverter-based-resources-cybersecurity.

Brown, Megan, Jacqueline Brown, Sydney White, and Joshua Waldman. “Calls for Cybersecurity Regulatory Harmonization Ramp Up in Congress, White House.” *Wiley* (blog), June 7, 2024. https://www.wiley.law/alert-Calls-for-Cybersecurity-Regulatory-Harmonization-Ramp-Up-in-Congress-White-House.

———. “CYBER UPDATE: White House Seeks Regulatory Harmonization While Exploring a Pilot for Reciprocity Amid Proliferation of Regulations.” *Wiley*, June 5, 2024. https://www.wiley.law/alert-CYBER-UPDATE-White-House-Seeks-Regulatory-Harmonization-While-Exploring-a-Pilot-for-Reciprocity-Amid-Proliferation-of-Regulations.

Critchley, Liam. “Old Becomes New: Retrofitting Legacy Equipment for Smart Grid.” *EE Power* (blog), May 14, 2024. https://eepower.com/tech-insights/old-becomes-new-retrofitting-legacy-equipment-for-smart-grid/#.

“Cyber Security for Distributed Energy Resources and DER Aggregators.” NERC, 2022. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf.

“Cyber Security: Understanding IEC 62351,” January 23, 2023. https://www.iec.ch/blog/cyber-security-understanding-iec-62351.

“Cybersecurity Baselines for Electric Distribution Systems and DER.” NARUC, February 2024. https://pubs.naruc.org/pub/35247A70-0C45-9652-C6D9-99A77C87200F?_gl=1*qhbmh7*_ga*MTA0MjA5NTEyNS4xNzI5NjA4NTc4*_ga_QLH1N3Q1NF*MTczMDI5NTQ4My4yLjAuMTczMDI5NTUxNS4wLjAuMA..

“Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid.” US Department of Energy, October 2022. https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf.

Gray, G. “Common Information Model (CIM)-MultiSpeak Harmonization 2nd Edition.” Technical. Palo Alto, CA: EPRI, Devcember 2012. https://restservice.epri.com/publicdownload/000000000001026585/0/Product.

“Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems.” IEEE SA, n.d. https://sagroups.ieee.org/scc21/standards/ieee-std-1547-3-2007-revision-in-progress/.

“IEC 62351 – Cyber Security Series for the Smart Grid.” IEC, Active. https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/.

"IEC 62443 Standard: An Overview." Fortinet, n.d. https://www.fortinet.com/resources/cyberglossary/iec-62443.

Johnson, Jay, and Danish Saleem. "Distributed Energy Resource (DER) Cybersecurity Standards." Presented at the NLR Cybersecurity & Resilience Workshop, Denver, CO, October 9, 2017. https://www.NLR.gov/docs/fy18osti/70454.pdf.

Lian, Jamie, Teja Kuruganti, and Yan Liu. "Artificial Intelligence Tools Secure Tomorrow's Electric Grid," July 22, 2024. https://www.ornl.gov/news/artificial-intelligence-tools-secure-tomorrows-electric-grid.

Misbrener, Kelsey. "New UL Certification Works to Protect Solar Inverters from Cyberattacks." *Solar Power World* (blog), October 1, 2024. https://www.solarpowerworldonline.com/2024/10/new-ul-certification-solar-inverters-cyberattacks/.

Narang, David. "Highlights of IEEE Standard 1547-2018 Implementation Considerations." Presented at the Global Power System Transformation Consortium Webinar, September 21, 2021. https://www.NLR.gov/docs/fy21osti/81028.pdf.

Powell, Charisa, Konrad Hauck, Anuj Sanghvi, Adarsh Hasandka, Joshua Van Natta, and Tami Reynolds. "Guide to the Distributed Energy Resources Cybersecurity Framework." National Renewable Energy Laboratory, December 2019. https://www.NLR.gov/docs/fy20osti/75044.pdf.

"Privacy and Security Impacts of DER and DER Aggregators." NERC, September 2023. https://www.nerc.com/comm/RSTC_Reliability_Guidelines/JointWhitePaper_PrivacyAndSecurityImpactsOfDERAggregators.pdf.

"Protecting Our Power: Cybersecurity Standards for Distributed Energy Resources." *IEEE SA*, December 12, 2024. https://standards.ieee.org/beyond-standards/cybersecurity-standards-der/.

Reed, Jonathan. "Regulatory Harmonization in OT-Critical Infrastructure Faces Hurdles." *IBM*, June 17, 2024. https://www.ibm.com/think/news/regulatory-harmonization-ot-critical-infrastructure-hurdles.

Saleem, Danish. "Cybersecurity Standards for Distributed Energy Resources." *NLR.Gov*, n.d. https://www.NLR.gov/security-resilience/cybersecurity-standards.html.

"SECURING DISTRIBUTED ENERGY RESOURCES." NIST, n.d. https://www.nccoe.nist.gov/sites/default/files/legacy-files/es-iiot-fact-sheet.pdf.

Seldon, Matt. "Office of the National Cyber Director Releases Summary of 2023 Cybersecurity Regulatory Harmonization Request for Information," June 11, 2024. https://www.hstoday.us/subject-matter-areas/cybersecurity/office-of-the-national-cyber-director-releases-summary-of-2023-cybersecurity-regulatory-harmonization-request-for-information/.

Siira, Mark, William Rubin, and Rudi Schubert. "IEEE Standards for the Evolving Distributed Energy Resources (DER) Ecosystem." *IEEE SA*, November 9, 2021. https://standards.ieee.org/beyond-standards/ieee-standards-for-the-evolving-distributed-energy-resources-der-ecosystem/.

Simeone, Christina. “The Distribution Grid Gap on Cybersecurity.” *Kleinman Center for Energy Policy* (blog), June 19, 2018. https://kleinmanenergy.upenn.edu/commentary/blog/the-distribution-grid-gap-on-cybersecurity/.

“The NIST Cybersecurity Framework (CSF) 2.0.” NIST, February 26, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

Tullman-Botzer, Jennifer. “How to Overcome the Top Challenges of OT Security with Zero-Trust Access.” *Cyolo* (blog), August 15, 2023. https://cyolo.io/blog/how-to-overcome-ot-security-challenges-with-zero-trust-access.

“What Is IEC 62443?” In *Zpedia*. zscaler, n.d. https://www.zscaler.com/zpedia/what-is-iec-62443.

Appendix A: Standards Evaluated for Gap Analysis

Table 1. Table of Standards Used for Gap Analysis

Standards with Scope & Applicability, Coverage and Adoption Challenges

Standard/Current Rev.	Scope & Applicability	Coverage of DER-Specific Risks	Adoption Challenges
IEC 60870-5 Series 2013	Telecontrol protocols for SCADA and DER integration; foundational for grid comms.	Limited-lacks robust security/authentication for distributed, internet-connected DERs.	Legacy protocol: upgrading to secure versions is costly and complex.
IEC 62270 / IEEE 1249 2013	Guide for hydro plant automation and computer-based control; covers DER control.	Addresses automation, control, and data acquisition, but not DER cybersecurity in depth.	Not DER-specific; limited guidance for modern DER cyber threats.
IEC 62351 Variable based on subsection,	Security for power system communication protocols (IEC 61850, 60870-5, etc.).	Strong focus on secure comms, encryption, authentication, and system management for DERs.	Complex; challenging integration with legacy systems; requires expertise for full implementation.
IEEE 1686-2022 2022	Cybersecurity for Intelligent Electronic Devices (IEDs) in power systems.	Device-level controls: access, config, firmware, data retrieval-relevant to DER IEDs.	Implementation in legacy devices is difficult; vendor support varies.
IEEE 1547.3-2023 2023	Cybersecurity guidance for DERs interconnected to electric power systems.	Comprehensive: risk assessment, access, data protection, network security for DERs.	New; requires redesign, new testing, and workforce training.
IEEE C37.240 2014	Cybersecurity for substation automation, protection, and control systems.	Focus on substations; some relevance for DERs at substation level.	May not address all DER-specific scenarios; integration with DER systems may be limited.
IEEE P2658 2022	Guide for cybersecurity testing in electric power systems, including DERs.	Provides test/verification methods for DER cybersecurity controls and protocols.	Still in draft, adoption depends on finalization and industry uptake.
IEEE P2808 2019	Machine-readable cybersecurity/communications parameters for engineering design.	Integrates cyber-by-design into DER engineering packages; supports documentation.	New approach requires changes to design workflows and toolchains.
ISA TR84.00.09 2017	Cybersecurity integration with functional safety lifecycle (SIS, alarms, controls).	Addresses cyber risks in safety systems; relevant for DERs with safety-critical functions.	Not DER-specific; complexity in integrating safety and cyber processes.
IEC 62443 Variable base on subsection.	Comprehensive IACS cybersecurity framework; widely used in OT/DER environments.	Defense-in-depth, zones/conduits, lifecycle security-applicable to DERs.	Complex, resource-intensive; challenging for small orgs and legacy DERs.

Standard/Current Rev.	Scope & Applicability	Coverage of DER-Specific Risks	Adoption Challenges
ISO/IEC 27019:2017 2017	Information security controls for energy utilities, including DER management.	Sector-specific ISMS for DERs; covers IT/OT convergence, risk management.	Requires mature ISMS; adaptation to DER operational realities may be needed.
ISO/SAE 21434:2021 2021	Cybersecurity for road vehicles and EVs; relevant to DERs in automotive context.	Focus on lifecycle cyber risk for EVs, V2G, and charging infrastructure.	Automotive focus: DER-specific adaptation required.
NERC CIP 2014	Mandatory cyber standards for BES; increasingly relevant to DERs via aggregators.	Focus on BES assets; DERs relevant if aggregated/impact BES reliability.	Not tailored for DERs; compliance for small DERs is challenging.
UL 2900-1 2023	Cybersecurity for network-connectable products (e.g., inverters, storage, EVSE).	Device-level security: secure development, vulnerability management, incident response.	Product certification can be costly; may require design changes.
UL 2941 2023	Cybersecurity requirements for DER and inverter-based resources (PV, EV, wind, etc.)	Security-by-design, device-level risks, testable certification for DER/IBR products.	New compliance requires product redesign and investment in certification.